EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2	(circuit and dummy and (permut$3 permutating)).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/21 18:27
S1	1	("20020083330").PN.	US-PGPUB; USPAT	OR	OFF	2007/06/21 18:26
S2	16	dummy adj circuit with (combin$3 encrypt$3 scrambl$3 encipher$4 encod$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/08 20:53
S3	126	code adj obfuscat$4	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/08 20:57
S4	2727	((326/8) or (703/13) or (703/15) or (713/187) or (713/190) or (716/4)).CCLS.	USPAT	OR	OFF	2007/06/21 13:55
S5	289	S4 and (@pd > "20051117")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/08 20:58
S7	1	("5748741").PN.	US-PGPUB; USPAT	OR	OFF	2006/06/09 14:03
S8	1	("6088452").PN.	US-PGPUB; USPAT	OR	OFF	2006/06/09 14:03
S9	4199	((326/8) or (703/13) or (703/15) or (713/187) or (713/190) or (716/4)).CCLS.	US-PGPUB; USPAT	OR	OFF	2006/10/03 12:10
S10	7086119	S9 an d(@pd > "20060609")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/21 15:38

EAST Search History

S11	305	S9 and (@pd > "20060609")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/03 12:31
S12	6588	(scrambl$3 encrypt$3) near4 circuit	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/03 12:32
S13	4731	(scrambl$3 encrypt$3) near2 circuit	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/03 12:32
S14	113	(scrambl$3 encrypt$3) near2 circuit same (dummy decoy false redundant)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/03 12:40
S15	13	((scrambl$3 encrypt$3) near2 circuit same (dummy decoy false redundant)).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/03 12:43
S16	1043	(713/189).CCLS.	US-PGPUB; USPAT	OR	OFF	2006/10/03 12:43
S17	176	S16 and (encrypt$3 scrambl$3) with circuit	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/03 12:43
S18	4730	((326/8) or (703/13) or (703/15) or (713/187) or (713/190) or (716/4)). CCLS.	US-PGPUB; USPAT	OR	OFF	2007/06/21 13:55
S19	531	S18 and (@pd > "20061003")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/21 14:45

EAST Search History

S20	38	circuit with (obfuscatation obfuscat$3 encrypt$3 scramb$3 encipher$3) same (fradulent dummy false) near4 (logic circuit code)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/21 15:33
S21	9	circuit with (permutat$3) same (fradulent dummy false) near4 (logic circuit code)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/21 15:33
S22	9	circuit with (permutat$3 permute) same (fradulent dummy false) near4 (logic circuit code)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/21 15:33
S23	10	circuit with (permutat$3 permut$3) same (fradulent dummy false) near4 (logic circuit code)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/21 15:33
S24	3	(((fake fradulent false dummy) adj circuit) with (encrypt$3 scrambl$3 obfuscat$3)).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/21 15:39

Terms used: **encryption obfuscation circuit dummy** Found **64** of **204,472**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window
Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 64 Result page: **1** 2 3 4 next

Relevance scale

1 Intrusion detection: Evading network anomaly detection systems: formal reasoning and practical techniques
Prahlad Fogla, Wenke Lee
October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**
Publisher: ACM Press
Full text available: pdf(288.16 KB) Additional Information: full citation, abstract, references, index terms

Attackers often try to evade an intrusion detection system (IDS) when launching their attacks. There have been several published studies in evasion attacks, some with available tools, in the research community as well as the "hackers" community. Our recent empirical case study showed that some payload-based network anomaly detection systems can be evaded by a polymorphic blending attack (PBA). The main idea of a PBA is to create each polymorphic instance in such a way that the statistics of att ...

Keywords: anomaly detection, mimicry attack, polymorphic blending attack

2 Multiagent systems and electronic markets track: Practical secrecy-preserving, verifiably correct and trustworthy auctions
D. C. Parkes, M. O. Rabin, S. M. Shieber, C. A. Thorpe
August 2006 **Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet ICEC '06**
Publisher: ACM Press
Full text available: pdf(507.45 KB) Additional Information: full citation, abstract, references, index terms

We present a practical system for conducting sealed-bid auctions that preserves the secrecy of the bids while providing for verifiable correctness and trustworthiness of the auction. The auctioneer must accept all bids submitted and follow the published rules of the auction. No party receives any useful information about bids before the auction closes and no bidder is able to change or repudiate her bid. Our solution uses Paillier's homomorphic encryption scheme [25] for zero knowledge proofs of ...

3 Applied cryptography II: Secure function evaluation with ordered binary decision diagrams
Louis Kruger, Somesh Jha, Eu-Jin Goh, Dan Boneh

October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**
Publisher: ACM Press
Full text available: pdf(302.55 KB) Additional Information: full citation, abstract, references, index terms

Privacy-preserving protocols allow multiple parties with private inputs to perform joint computation while preserving the privacy of their respective inputs. An important cryptographic primitive for designing privacy-preserving protocols is secure function evaluation (SFE). The classic solution for SFE by Yao uses a gate representation of the function that the two parties want to jointly compute. Fairplay is a system that implements the classic solution for SFE. In this paper, we present a new p ...

Keywords: binary decision diagrams, secure function evaluation

4 Masking the Energy Behavior of DES Encryption
H. Saputra, N. Vijaykrishnan, M. Kandemir, M. J. Irwin, R. Brooks, S. Kim, W. Zhang
March 2003 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 1 DATE '03**
Publisher: IEEE Computer Society
Full text available: pdf(264.41 KB) Publisher Site Additional Information: full citation, abstract, citings, index terms

Smart cards are vulnerable to both invasive and non-invasive attacks. Specifically, non-invasive attacks using power and timing measurements to extract the cryptographic key has drawn a lot of negative publicity for smart card usage. The power measurement techniques rely on the data-dependent energy behavior of the underlying system. Further, power analysis can be used to identify the specific portions of the program being executed to induce timing glitches that may in turn help to bypass key ch ...

5 A database encryption system with subkeys
George I. Davida, David L. Wells, John B. Kam
June 1981 **ACM Transactions on Database Systems (TODS)**, Volume 6 Issue 2
Publisher: ACM Press
Full text available: pdf(1.16 MB) Additional Information: full citation, abstract, references, citings, index terms

A new cryptosystem that is suitable for database encryption is presented. The system has the important property of having subkeys that allow the encryption and decryption of fields within a record. The system is based on the Chinese Remainder Theorem.

Keywords: data security, databases, decryption, encryption, subkeys

6 Session 3A: markets and auctions II: Secure multi-agent dynamic programming based on homomorphic encryption and its application to combinatorial auctions
Makoto Yokoo, Koutarou Suzuki
July 2002 **Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1 AAMAS '02**
Publisher: ACM Press
Full text available: pdf(181.62 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper presents a secure dynamic programming protocol that utilizes homomorphic encryption. By using this method, multiple agents can solve a combinatorial optimization problem among them without leaking their private information. More specifically, in this method, multiple servers cooperatively perform dynamic programming procedures for

solving a combinatorial optimization problem by using the private information sent from agents as inputs. Although the severs can compute the optimal soluti ...

Keywords: auction, dynamic programming, electronic commerce, privacy, public key encryption, security and agents

7 Privacy-preserving credit checking

Keith Frikken, Mikhail Atallah, Chen Zhang

June 2005 **Proceedings of the 6th ACM conference on Electronic commerce EC '05**

Publisher: ACM Press

Full text available: pdf(166.37 KB) Additional Information: full citation, abstract, references, index terms

Typically, when a borrower (Bob) wishes to establish a tradeline (e.g., a mortgage, an automobile loan, or a credit card) with a lender (Linda), Bob is subjected to a credit check by Linda. The credit check is done by having Linda obtain financial information about Bob in the form of a credit report. Credit reports are maintained by Credit Report Agencies, and contain a large amount of private information about individuals. Furthermore, Linda's criteria for loan qualification are also private in ...

Keywords: e-commerce, privacy, secure multi-party computation, secure protocol

8 Routing: ANODR: anonymous on demand routing with untraceable routes for mobile ad-hoc networks

Jiejun Kong, Xiaoyan Hong

June 2003 **Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing MobiHoc '03**

Publisher: ACM Press

Full text available: pdf(236.79 KB) Additional Information: full citation, abstract, references, citings, index terms

In hostile environments, the enemy can launch traffic analysis against interceptable routing information embedded in routing messages and data packets. Allowing adversaries to trace network routes and infer the motion pattern of nodes at the end of those routes may pose a serious threat to covert operations. We propose ANODR, an anonymous on-demand routing protocol for mobile ad hoc networks deployed in hostile environments. We address two closely related problems: For *route anonymity*, AN ...

Keywords: anonymity, broadcast, mobile ad-hoc network, on-demand routing, pseudonymity, trapdoor, untraceability

9 Design and implementation of a scalable encryption processor with embedded variable DC/DC converter

James Goodman, Anantha Chandrakasan, Abram P. Dancy

June 1999 **Proceedings of the 36th ACM/IEEE conference on Design automation DAC '99**

Publisher: ACM Press

Full text available: pdf(119.51 KB) Additional Information: full citation, references, citings, index terms

10 Information flow: Private inference control

David Woodruff, Jessica Staddon

October 2004 **Proceedings of the 11th ACM conference on Computer and**

communications security CCS '04
Publisher: ACM Press

Full text available: pdf(269.55 KB) Additional Information: full citation, abstract, references, citings, index terms

Access control can be used to ensure that database queries pertaining to sensitive information are not answered. This is not enough to prevent users from learning sensitive information though, because users can combine non-sensitive information to discover something sensitive. Inference control prevents users from obtaining sensitive information via such "inference channels", however, existing inference control techniques are not private - that is, they require the server to learn what querie ...

Keywords: inference control, oblivious transfer, private information retrieval

11 Design Method for Constant Power Consumption of Differential Logic Circuits

Kris Tiri, Ingrid Verbauwhede
March 2005 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 1 DATE '05**
Publisher: IEEE Computer Society
Full text available: pdf(146.44 KB) Additional Information: full citation, abstract, index terms

Side channel attacks are a major security concern for smart cards and other embedded devices. They analyze the variations on the power consumption to find the secret key of the encryption algorithm implemented within the security IC. To address this issue, logic gates that have a constant power dissipation independent of the input signals, are used in security ICs. This paper presents a design methodology to create fully connected differential pull down networks. Fully connected differential pul ...

12 Trust, access control and privacy: Achieving privacy in mesh networks

Xiaoxin Wu, Ninghui Li
October 2006 **Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks SASN '06**
Publisher: ACM Press
Full text available: pdf(449.10 KB) Additional Information: full citation, abstract, references, index terms

Mesh network is vulnerable to privacy attacks because of the open medium property of wireless channel, the fixed topology, and the limited network size. Traditional anonymous routing algorithm cannot be directly applied to Mesh network, because they do not defend global attackers. In this paper we design private routing algorithm that used "Onion", i.e., layered encryption, to hide routing information. In addition, we explore special ring topology that fits the investigated network scenario, to ...

Keywords: mesh networks, privacy

13 Encryption-based protection for interactive user/computer communication

Stephen Thomas Kent
September 1977 **Proceedings of the fifth symposium on Data communications SIGCOMM '77**
Publisher: ACM Press
Full text available: pdf(846.33 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper develops a virtual connection model, complete with intruder, for interactive terminal-host communication and presents a set of protection goals that characterize the security that can be provided for a physically unsecured connection. Fundamental requirements for protocols that achieve these goals and the role of encryption in the

design of such protocols are examined. Functional and security constraints on positioning of protection protocols in a communication system and the imp ...

14 Security on FPGAs: State-of-the-art implementations and attacks

Thomas Wollinger, Jorge Guajardo, Christof Paar

August 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 3

Publisher: ACM Press

Full text available: pdf(296.79 KB) Additional Information: full citation, abstract, references, index terms

In the last decade, it has become apparent that embedded systems are integral parts of our every day lives. The wireless nature of many embedded applications as well as their omnipresence has made the need for security and privacy preserving mechanisms particularly important. Thus, as field programmable gate arrays (FPGAs) become integral parts of embedded systems, it is imperative to consider their security as a whole. This contribution provides a state-of-the-art description of security issues ...

Keywords: Cryptography, FPGA, attacks, cryptographic applications, reconfigurable hardware, reverse engineering, security

15 Non-reversible VHDL source-source encryption

Kevin O'Brien, Serge Maginot

September 1994 **Proceedings of the conference on European design automation EURO-DAC '94**

Publisher: IEEE Computer Society Press

Full text available: pdf(678.63 KB) Additional Information: full citation, references, citings, index terms

16 Cryptography and data security

Dorothy Elizabeth Robling Denning

January 1982 Book

Publisher: Addison-Wesley Longman Publishing Co., Inc.

Full text available: pdf(19.47 MB) Additional Information: full citation, abstract, references, citings, index terms

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prolific practical data processing systems in the 1980s. As we have come to rely on these systems to process and store data, we have also come to wonder about their ability to protect valuable data.

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure ...

17 Power Attack Resistant Cryptosystem Design: A Dynamic Voltage and Frequency Switching Approach

Shengqi Yang, Wayne Wolf, N. Vijaykrishnan, D. N. Serpanos, Yuan Xie

March 2005 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 3 DATE '05**

Publisher: IEEE Computer Society

Full text available: pdf(291.83 KB) Additional Information: full citation, abstract, index terms

A novel power attack resistant cryptosystem is presented in this paper. Security in digital computing and communication is becoming increasingly important. Design techniques that

can protect cryptosystems from leaking information have been studied by several groups. Power attacks, which infer program behavior from observing power supply current into a processor core, are important forms of attacks. Various methods have been proposed to countermeasure the popular and efficient power attacks. Howe ...

18 Verification and security: Policy-hiding access control in open environment

Jiangtao Li, Ninghui Li

July 2005 **Proceedings of the twenty-fourth annual ACM symposium on Principles of distributed computing PODC '05**

Publisher: ACM Press

Full text available: pdf(247.72 KB) Additional Information: full citation, abstract, references, citings, index terms

In trust management and attribute-based access control systems, access control decisions are based on the attributes (rather than the identity) of the requester: Access is granted if Alice's attributes in her certificates satisfy Bob's access control policy. In this paper, we develop a policy-hiding access control scheme that protects both sensitive attributes and sensitive policies. That is, Bob can decide whether Alice's certified attribute values satisfy Bob's policy, without Bob learning any ...

Keywords: access control, automated trust negotiation, cryptographic commitment, cryptographic protocol, digital credentials, evaluation, privacy, secure function

19 The development and proof of a formal specification for a multilevel secure system

Janice I. Glasgow, Glenn H. MacEwen

March 1987 **ACM Transactions on Computer Systems (TOCS)**, Volume 5 Issue 2

Publisher: ACM Press

Full text available: pdf(2.62 MB) Additional Information: full citation, abstract, references, citings, index terms, review

This paper describes current work on the design and specification of a multilevel secure distributed system called SNet. It discusses security models in general, the various problems of information flows in SNet, and the abstract and concrete security model components for SNet. It also introduces Lucid as a language for specifying distributed systems. The model components are expressed in Lucid; these Lucid partial specifications are shown to be correct with respect to the formal model, and ...

20 Sensor networks (work in progress): Mobile traffic sensor network versus motion-MIX: tracing and protecting mobile wireless nodes

Jiejun Kong, Dapeng Wu, Xiaoyan Hong, Mario Gerla

November 2005 **Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks SASN '05**

Publisher: ACM Press

Full text available: pdf(374.84 KB) Additional Information: full citation, abstract, references, index terms

In this paper we focus on passive attacks that threaten the privacy of mobile wireless networks. We define the concept of "venue privacy attack" (VPA) to illustrate the emerging anonymity attacks to trace mobile wireless nodes. Then we propose "motion-MIX" as the countermeasure to defend against various venue privacy attacks. We study the necessary conditions to implement motion-MIXes. These conditions include identity-free routing, one-time packet content and various other concerns in the netwo ...

Keywords: ANODR, anonymity, identity-free routing, mobility, motion-MIX